

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X	:	
	:	
IN RE CHRISTIE’S DATA BREACH LITIGATION,	:	24-CV-4221 (JMF)
	:	
<i>This Document Relates To:</i>	:	<u>MEMORANDUM OPINION</u>
<i>All Member Cases</i>	:	<u>AND ORDER</u>
	:	
-----X	:	

JESSE M. FURMAN, United States District Judge:

On May 8, 2024, cybercriminals hacked and stole data maintained by Christie’s Inc. (“Christie’s”), the well-known auction house. ECF No. 43 (“FAC”), ¶¶ 17, 22-23. The stolen data included the personal identifiable information (“PII”) of Christie’s customers, including full names, birthdates, addresses, passport numbers, and driver’s license numbers. *Id.* ¶¶ 3, 24-25. Thereafter, some of those whose PII had been compromised brought this putative class action against Christie’s, alleging, in substance, that Christie’s had violated its obligations to them by inadequately protecting their data. *Id.* ¶¶ 173-272. Christie’s moved to dismiss, arguing, among other things, that Plaintiffs lacked standing under Article III of the U.S. Constitution. *See* ECF Nos. 40, 44. Before the motion was resolved, however, the parties reached a class-wide settlement and jointly moved to stay all deadlines pending a motion, pursuant to Rule 23(e) of the Federal Rules of Civil Procedure, for preliminary approval of that settlement. *See* ECF No. 47. Plaintiffs followed with a motion. *See* ECF No. 49. Mindful of Christie’s earlier motion to dismiss and the Court’s obligation to assure itself of its jurisdiction even in this setting, *see Frank v. Gaos*, 586 U.S. 485, 492 (2019) (per curiam), the Court ordered the parties to submit supplemental memoranda of law addressing the issue of standing, ECF No. 50; *see also* ECF No. 55. Having reviewed the parties’ submissions, *see* ECF Nos. 51, 52, 56, the Court

concludes that Plaintiffs do have Article III standing and, with one caveat, grants the motion for preliminary approval of the class action settlement.

The general principles that govern Article III standing are well established. Most relevant here, to have standing, a plaintiff must demonstrate a “judicially cognizable injury in fact,” *Schulz v. Williams*, 44 F.3d 48, 52 (2d Cir. 1994) (internal quotation marks omitted), that is both “concrete and particularized” and “actual or imminent,” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). An injury is “concrete” if it “has a ‘close relationship’ to a harm traditionally recognized as providing a basis for a lawsuit in American courts,” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 417 (2021) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)), and “particularized” if it “affect[s] the plaintiff in a personal and individual way,” *Spokeo, Inc.*, 578 U.S. at 339. By contrast, an injury is not particularized if it is a “grievance . . . suffer[ed] . . . in common with people generally.” *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 344 (2006) (internal quotation marks omitted). Meanwhile, an “actual” injury is one that has “already occurred,” *Food & Drug Admin. v. All. for Hippocratic Med.*, 602 U.S. 367, 381 (2024); *see also Soule v. Conn. Ass’n of Schs., Inc.*, 90 F.4th 34, 46 (2d Cir. 2023) (en banc) (“[A]n injury is actual . . . if it has actually happened” (internal quotation marks omitted)), while an “imminent” injury is a “future injury” that is nonetheless “certainly impending,” with a “substantial risk” of occurrence, *Lacewell v. Off. of Comptroller of Currency*, 999 F.3d 130, 141 (2d Cir. 2021) (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)).

In two recent cases that loom large here, the Second Circuit has applied these principles to claims involving the exposure of PII. First, in *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021), a health services provider inadvertently sent a company-wide email with an attached spreadsheet containing employee PII. *See id.* at 298. A group of employees

filed a class action arguing they were “at imminent risk of . . . identity theft” from the misfired email. *Id.* In concluding the employees lacked standing, the court identified three “factors” that, while absent in that case, could “weigh in favor of finding an Article III injury in fact” in another data breach case. *Id.* at 301. The first factor is “whether the data at issue has been compromised as the result of a targeted attack intended to obtain the plaintiffs’ data.” *Id.* The second is whether “at least some part of the compromised dataset has been misused.” *Id.* The third “look[s] to the type of data at issue, and whether that type of data is more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed.” *Id.* at 302. In particular, the court observed that “the dissemination of high-risk information such as Social Security numbers and dates of birth — especially when accompanied by victims’ names — makes it more likely that those victims will be subject to future identity theft or fraud. By contrast, less sensitive data, such as basic publicly available information, or data that can be rendered useless to cybercriminals does not pose the same risk of future identity theft or fraud to plaintiffs if exposed.” *Id.* (citation omitted).

More recently, in *Bohnak v. Marsh & McLennan Companies, Inc.*, 79 F.4th 276 (2d Cir. 2023), the Second Circuit reevaluated the “continuing vitality” of the *McMorris* factors in light of the Supreme Court’s intervening decision in *TransUnion LLC v. Boix*. *Bohnak*, 79 F.4th at 283. The court held that *TransUnion* was “the touchstone for determining whether [the plaintiff] ha[d] alleged a concrete injury,” *id.*, but that “the *McMorris* framework continues to apply” to the determination of whether “an injury arising from risk of future harm” in a data breach case “is ‘actual or imminent,’” *id.* at 280. Notably, the court then concluded that the plaintiff — whose PII had been stolen by cybercriminals — had standing for two distinct reasons. First, the court concluded that she had standing because she had “been harmed by the exposure of her private

information . . . to an unauthorized malevolent actor.” *Id.* at 286. That harm — already suffered by the plaintiff — was similar enough to the “‘disclosure of private information,’ . . . an “intangible harm ‘traditionally recognized as providing a basis for lawsuits in American courts,’” to support standing. *Id.* (quoting *TransUnion*, 594 U.S. at 425). Second, the plaintiff “suffered ‘separate concrete harm[s],’” *id.* (quoting *TransUnion*, 594 U.S. at 436) — including “out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft” — “as a result of the risk of future harm occasioned by the exposure of her PII,” *id.* Significantly, the court subjected only this second form of injury to analysis under *McMorris*. *Id.* at 285.

Applying *Bohnak* and *McMorris* to the claims in this case, the Court concludes that Plaintiffs allege injuries that are both “concrete” and “actual or imminent.” First, like the plaintiff in *Bohnak*, Plaintiffs here allege that they have already been harmed by the disclosure of their private information to an unauthorized malevolent actor. *See, e.g.*, FAC ¶¶ 34, 40, 43. That injury is plainly “concrete.” *See Bohnak*, 79 F.4th at 285-86. And because it is “has actually happened,” *Soule*, 90 F.4th at 46, it need not be analyzed using the *McMorris* factors. In so holding, the Court admittedly parts ways with some district courts in this Circuit, which have read *Bohnak* to say that “the disclosure of [] PII to a fraudulent actor” suffices only if it also passes muster under *McMorris*. *Cantinieri v. Verisk Analytics, Inc.*, No. 21-CV-6911 (NJC) (JMW), 2024 WL 5202579, at *11 (E.D.N.Y. Dec. 23, 2024); *accord Addi v. Int’l Bus. Machines, Inc.*, No. 23-CV-5203 (NSR), 2024 WL 2802863, at *4 (S.D.N.Y. May 31, 2024); *but see Eletson Holdings, Inc. v. Levona Holdings Ltd.*, 731 F. Supp. 3d 531, 573 (S.D.N.Y. 2024) (“The Second Circuit has held, post-*TransUnion*, that a plaintiff whose private information has been disclosed to third parties has standing to sue regardless of whether the third parties used that information to cause additional harm.” (citing *Bohnak*, 79 F.4th at 285-86)); *Jones v. Sturm*,

Ruger & Co., Inc., No. 22-CV-1233 (KAD), 2024 WL 1307148, at *3 (D. Conn. Mar. 27, 2024) (engaging in the “actual or imminent” inquiry only for the second *Bohnak* injury). That reading overlooks the fact that the *Bohnak* court applied the *McMorris* factors only to the plaintiff’s second form of injury, arising from the “risk of future harm.” *Bohnak*, 79 F.4th at 286; *see also id.* at 288 (stating that the *McMorris* factors “shed light on whether the future harm of identity theft or fraud resulting from a data breach is sufficiently actual and imminent”). Nor can it be reconciled with *Salazar*, in which the Second Circuit applied *Bohnak*’s holding that public disclosure is itself a cognizable injury without any analysis of whether that already completed disclosure was “actual or imminent.” *See Salazar*, 118 F.4th at 541-42.¹

That is enough to conclude that Plaintiffs in this case have standing. But, as in *Bohnak*, Plaintiffs here “establish a concrete injury for purposes of [their] damages claim[s] for a separate reason”: They allege that they have expended “significant time and effort,” FAC ¶ 55, and “out of pocket costs,” *id.* ¶ 135, to mitigate the risks posed by the data breach. *Bohnak*, 79 F.4th at 286. This type of injury *is* subject to analysis using the *McMorris* factors, which makes the question of whether it supports standing a closer call than Plaintiffs’ first type of injury. But the Court concludes that it too suffices. The first *McMorris* factor plainly supports that conclusion, as it is undisputed that Christie’s was “hacked by cybercriminals” who “exfiltrated” PII from its systems. FAC ¶¶ 22-23. The second factor, by contrast, is more equivocal. True, Plaintiffs allege “cybercriminals attempted to hack into [one Plaintiff’s] cell phone account” and

¹ Application of the *McMorris* factors to the second injury identified in *Bohnak* also makes sense in light of the Supreme Court’s decision in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), which held that a plaintiff “cannot manufacture standing by incurring costs in anticipation of *non-imminent* harm,” *id.* at 422 (emphasis added). By contrast, that admonition does not apply to the first type of injury — the public disclosure of private information — which is not self-inflicted, let alone self-inflicted in anticipation of a future risk.

“attempted to hack into [another Plaintiff’s] PayPal account.” FAC ¶¶ 72, 125. But the PayPal hacking attempt appears to have occurred *before* the breach, *see* ECF No. 52, at 6, and it is unclear whether any attempted — but possibly unsuccessful, *compare* FAC ¶ 125, *with* ECF No. 51, at 2 — hacking of a cellphone was tied to the breach, *see, e.g.*, ECF No. 45, 13-15 (questioning the “temporal and logical connection between the Breach and [Plaintiffs’] injuries” (emphasis omitted)). And while Plaintiffs contend that publication of their data on the Dark Web “provide[s] strong support” for their claimed injury, *McMorris*, 995 F.3d at 302; FAC ¶¶ 40-43, the extent to which that is the case still turns on “the nature of the data itself,” *McMorris*, 995 F.3d at 304 n.6; *see also Cooper v. Bonobos, Inc.*, No. 21-CV-854 (JMF), 2022 WL 170622, at *3 (S.D.N.Y. Jan. 19, 2022) (explaining that “the third *McMorris* factor” can “doom[] [a plaintiff’s] ability to establish standing based on an increased risk of identity theft or fraud”).

Thus, whether Plaintiffs’ second type of injury independently supports standing ultimately turns on the final *McMorris* factor: whether the “type of data” stolen is “likely to subject plaintiffs to a perpetual risk of identity theft or fraud.” *McMorris*, 995 F.3d at 302; *Liau v. Weee! Inc.*, No. 23-CV-1177 (PAE), 2024 WL 729259, at *4 (S.D.N.Y. Feb. 22, 2024) (finding that the first and second *McMorris* factors — although “weigh[ing] in plaintiffs’ favor” — “ultimately merit[ed] little weight so as not to carry the day”). From the cases analyzing that factor, there emerges a rough spectrum based on the extent to which the exposed data “subject plaintiffs to a perpetual risk of identity theft or fraud.” *Id.* On one end of the spectrum are Social Security numbers, which are “among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.” *Bohnak*, 79 F.4th at 289. On the other end of the spectrum are “basic publicly available information” — that is, data that, while sensitive, “can be rendered useless to

cybercriminals,” *McMorris*, 995 F.3d at 302, such as “passwords” or “credit card numbers” for which a plaintiff could “take[] the simple step” of changing the password or “canceling the card.” *Cooper*, 2022 WL 170622, at *4; *see also McMorris*, 995 F.3d at 302.

The PII exfiltrated by the hackers in this case—which included “full names, passport information, driver’s license information, and state and government-issued ID information,” FAC ¶ 24—falls somewhere in the middle of the spectrum. Driver’s license numbers, for example, can be “difficult and highly problematic to change.” *Stallone v. Farmers Grp., Inc.*, No. 22-CV-01659 (GMN) (VCF), 2022 WL 10091489, at *5 (D. Nev. Oct. 15, 2022) (internal quotation marks omitted). Yet they are routinely altered when “people move to different states or licenses are renewed.” *Baysal v. Midvale Indem. Co.*, 78 F.4th 976, 979 (7th Cir. 2023). And driver’s license numbers are not as commonly associated with fraud and identity theft as Social Security numbers. It is perhaps for these reasons—and associated differences between different plaintiffs’ pleadings—that courts in this circuit appear divided on whether driver’s license numbers are the type of data that satisfies the third *McMorris* factor. *Compare, e.g., In re USAA Data Sec. Litig.*, 621 F. Supp. 3d 454, 466-67 (S.D.N.Y. 2022) (finding that stolen driver’s license numbers “can provide an opening for fraud,” especially when they are with “other personal information” that would allow those possessing them to “apply[] for credit cards or loans or open[] bank accounts”), *and Rand v. Travelers Indem. Co.*, 637 F. Supp. 3d 55, 67 (S.D.N.Y. 2022) (similar), *with Cantinieri*, 2024 WL 5202579, at *17 (observing that the plaintiffs had failed to allege “that the disclosure of” their driver’s license numbers could “provide an opening for fraud”). Plaintiffs here do not include allegations on this score in their operative complaint, but in their supplemental submissions they point to sources—statutes and government publications, of which the Court can take notice—indicating that stolen driver’s

license numbers can be “a gold mine for hackers” and “a critical part of a fraudulent, synthetic identity.” ECF No. 56, at 3-5; *see also id.* at 6 & n.6 (citing a “U.S. State Department warn[ing] of the dangers of passport fraud, including assuming identities or committing financial crimes and bank fraud”).² The Court concludes that this is sufficient to satisfy the third *McMorris* factor and, thus, that Plaintiffs’ second alleged form of injury suffices to support standing as well.

For the foregoing reasons, the Court concludes that it has subject-matter jurisdiction and, thus, may review Plaintiffs’ unopposed motion for preliminary approval of the parties’ proposed class action settlement. With one caveat, the Court finds, substantially for the reasons set forth in Plaintiffs’ submissions, *see* ECF Nos. 51, 56, that the proposed settlement warrants approval. The caveat pertains to the parties’ request that the Court stay “any actions brought by Settlement Class Members concerning the Released Claims . . . pending Final Approval of the Settlement Agreement.” ECF No. 49-3, ¶ 16; *see* ECF No. 51, at 12-13. The parties are not aware of any other such actions, which renders such a stay unnecessary. But even if the parties were aware of other such actions, the Court would decline to intrude on the “broad . . . discretion” of another court “to stay proceedings as an incident to its power to control its docket,” *Collazos v. United States*, 368 F.3d 190, 201 (2d Cir. 2004), including to await “resolution of independent legal proceedings” elsewhere, *Nat’l Indus. for Blind v. Dep’t of Veterans Affs.*, 296 F. Supp. 3d 131, 137 (D.D.C. 2017) (Jackson, J.). Nor would the Court interfere with other litigants’ rights

² *See, e.g.*, The Driver’s Privacy Protection Act, 18 U.S.C. §§ 2721 *et seq.*; *see also, e.g.*, N.Y. Dep’t Fin. Servs., *Re: Cyber Fraud Alert* (Feb. 16, 2021) (reporting that hackers have used driver’s license numbers to “submit fraudulent claims for pandemic and unemployment benefits”), <https://perma.cc/VBV3-CXEL>; U.S. Dep’t Treas. Fin. Crimes Enf’t Network, *FinCEN Notice on the Use of Counterfeit U.S. Passport Cards to Perpetrate Identity Theft and Fraud Schemes at Financial Institutions* (April 15, 2024), <https://perma.cc/LJN5-BL7U>.

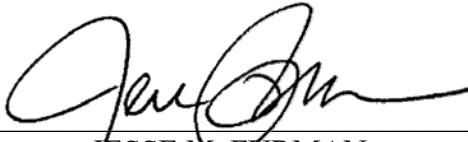
without giving them notice and an opportunity to be heard. Accordingly, the Court will strike that language from the parties' proposed order.

In sum, the Court GRANTS Plaintiffs' unopposed motion for preliminary approval of the parties' proposed class action settlement. The Court will enter an order preliminarily approving the settlement, with the amendment discussed above, separately.

The Clerk of Court is directed to terminate ECF No. 49.

SO ORDERED.

Dated: February 19, 2025
New York, New York



JESSE M. FURMAN
United States District Judge